DETAILED ACTION

1. This is in response to the amendment filed July 23, 2008. Claims 1-4, 7, 14 and 18 have been amended. Claims 5-6, 8-13, 15-17 and 19-21 have been cancelled. Claims 1-4, 7, 14 and 18 are pending and have been considered below.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Himanshu S. Amin, (Registration. No. 40,894) on 10/23/2008

The application has been amended as follows:

.

Claims

Please amend the claims as follows:.

1 (Currently Amended) A wireless network detection system including computer storage medium storing a computer executable instructions that when executed on one or more processors facilitates identification of wireless network encryption type, said system comprising:

a connection component that can connect a device to a plurality of wireless networks; and,

a detection component that automatically identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon eliminating one or more of a plurality of possible encryption types by at least one of detecting a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold ~~during~~ without having detected an expected portion of the authentication sequence of the available wireless network, wherein identifying the encryption type includes:

the detection component attempting an 802.1x authentication sequence to the wireless network and determining that the wireless network as a wired equivalent privacy network requiring a wired equivalent privacy key when a failure of a portion of the 802.1x authentication sequence or exceeding a time threshold without having detected an expected portion of the 802.1x authentication sequence occurs;

the detection component identifying the wireless network as a 802.1x when a failure of a portion of the 802.1x authentication sequence and exceeding a time threshold without having detected an expected portion of the 802.1x authentication sequence do not occur;

the detection component having identified the wireless network as a 802.1x attempting a wireless provisioning services sequence and determining that the wireless network does not support wireless provisioning services ~~when the wireless network supports 802.1x~~ when a failure of a portion of the wireless provisioning services authentication sequence or exceeding a time threshold without having detected an

expected portion of the wireless provisioning services authentication sequence occurs; and,

the detection component identifying the wireless network as a 802.1x supporting wireless provisioning services network when a ~~no~~ failure of a portion of the wireless provisioning services authentication sequence and exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence do not occur.

2. (Previously Presented) The system of claim 1, identification of the encryption type of the available wireless network by the detection component being based, at least in part, upon receipt of an information element from a wireless network beacon.

3. (Previously Presented) The system of claim 1, the available wireless network comprising at least one of an unencrypted network, a Wired Equivalent Privacy (WEP) network requiring a WEP key, a Wi-Fi Protected Access (WPA) encrypted network requiring a WPA pre-shared key, an 802.1x-enabled network that does not support WPA, an 802.1x-enabled network that does support WPA and a wireless provisioning services (WPS) support-enabled network.

4. (Previously Presented) The system of claim 1, identification of the encryption type of the available wireless network by the detection component being based, at least in part, upon iterative probing of the available network.

5. (Previously Presented) The system of claim 4, wherein the detection component attempts to connect to the available wireless network as a wireless provisioning services-supporting network, the detection component determining that the available wireless network is a pre-shared key network if a failure in an authentication sequence from a wireless network beacon is determined.

6. (Previously Presented) The system of claim 5, the detection component determining that the available wireless network is a Wi-Fi Protected Access network if a failure in a particular piece of the authentication sequence that identifies a wireless provisioning services supporting network is determined.

7. (Original) The system of claim 6, the particular piece of the authentication sequence comprising a type, length value sequence.

8. (Previously Presented) The system of claim 6, the detection component determining that the available wireless network is a wireless provisioning services supporting network if the particular piece of authentication sequence identifying the wireless provisioning services supporting network is received from the wireless network beacon.

9. (Previously Presented) The system of claim 1, wherein the detection component sends at least one of a connect message, an 802.1x Extensible Authentication Protocol Over Lan (EAPOL) start message, an 802.1x identity message.

10. (Original) The system of claim 1, wherein the detection component receives at least one of an associated message, an 802.1x identity request message, an authentication message and a provisioning message from a wireless network beacon.

11-14. (Cancelled)

15. (Currently Amended) A method facilitating wireless network detection comprising:

determining whether a wireless network supports 802.1x by attempting an 802.1x authentication sequence to the wireless network;[[,]]

identifying the wireless network as a wired equivalent privacy network requiring a wired equivalent privacy key when a failure of a portion of the 802.1x authentication sequence or exceeding a time threshold without having detected an expected portion of the 802.1x authentication sequence occurs;

identifying the wireless network as a 802.1x when a failure of a portion of the 802.1x authentication sequence and exceeding a time threshold without having detected an expected portion of the 802.1x authentication sequence do not occur;

having identified the wireless network as a 802.1x attempting a wireless provisioning services sequence;

identifying the wireless network as a 802.1x that does not support wireless provisioning services when a failure of a portion of the wireless provisioning services authentication sequence or exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence occurs; and,

identifying the wireless network as a 802.1x supporting wireless provisioning services network when a failure of a portion of the wireless provisioning services authentication sequence and exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence do not occur.

~~based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence~~;

~~identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key when the wireless network does not support 802.1x;~~

~~determining whether the wireless network supports wireless provisioning services when the wireless network supports 802.1x based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; and,~~

~~identifying the wireless network as an 802.1x network when the wireless network does not support wireless provisioning services; and,~~

~~identifying the wireless network as a wireless provisioning services supporting network when the wireless network supports wireless provisioning services.~~

16. (Currently Amended) The method of claim 15, further comprising at least one of the following acts:

determining whether the wireless network is encryption enabled;

upon determining that the wireless network is encrypted, determining if ~~whether~~ the wireless network is a Wi-Fi Protected Access (WPA~~WAP~~) network; and,

upon determining that the wireless network is a Wi-Fi Protected Access (WPA) network, identifying the network as a WPA network and determining whether the WPA wireless network is a Wi-Fi Protected Access (WPA~~WAP~~) pre-shared key network; and

17. (Currently Amended) The method of claim 16, further comprising at least one of the following acts:

identifying the wireless network as unencrypted, ~~if~~ upon determining the wireless network is not encryption enabled; and,

identifying the wireless network as a Wi-Fi Protected Access pre-shared key network, upon determining the WPA wireless network is a Wi-Fi Protected Access (WPA) pre-shared key network.

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (Currently Amended) A wireless network detection system including computer storage medium storing a computer executable instructions that when executed on one or more processors facilitates identification of wireless network encryption type, said system comprising:

means for connecting a device to a plurality of wireless networks; and,

means for automatically identifying an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon eliminating one or more of a plurality of possible encryption types by at least one of detecting at least one of failure of a portion of an authentication sequence or exceeding a time threshold without having detected a particular portion of the authentication sequence, wherein identifying the encryption type includes:

means for automatically identifying an encryption type attempting an 802.1x authentication sequence to the wireless network and determining that the wireless network as a wired equivalent privacy network requiring a wired equivalent privacy key when a failure of a portion of the 802.1x authentication sequence or exceeding a time

threshold without having detected an expected portion of the 802.1x authentication sequence occurs;

means for automatically identifying an encryption type identifying the wireless network as a 802.1x when a failure of a portion of the 802.1x authentication sequence and exceeding a time threshold without having detected an expected portion of the 802.1x authentication sequence do not occur;

means for automatically identifying an encryption type having identified the wireless network as a 802.1x attempting a wireless provisioning services sequence and determining that the wireless network does not support wireless provisioning services when a failure of a portion of the wireless provisioning services authentication sequence or exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence occurs; and,

means for automatically identifying an encryption type identifying the wireless network as a 802.1x supporting wireless provisioning services network when a failure of a portion of the wireless provisioning services authentication sequence and exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence do not occur.

Allowance

Claims 1-10, 15-17 and 22 have amended with written arguments, which overcome the examiner's prior art rejection see argument of July 21, 2008. The examiner withdraws all outstanding rejections.

Examiner's Statement of reason of Allowance

The prior art references of record do not teach or render obvious the limitations as recited in independent claims 1, 15 and 22 specific to include a connection component that can connect a device to a plurality of wireless networks; and, a detection component that automatically identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon eliminating one or more of a plurality of possible encryption types by at least one of detecting a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold without having detected an expected portion of the authentication sequence of the available wireless network, wherein identifying the encryption type includes: the detection component attempting an 802.1x authentication sequence to the wireless network and determining that the wireless network as a wired equivalent privacy network requiring a wired equivalent privacy key when a failure of a portion of the 802.1x authentication sequence or exceeding a time threshold without having detected an expected portion of the 802.1x authentication sequence occurs; the detection component identifying the wireless network as a 802.1x when a failure of a portion of the 802.1x authentication sequence and exceeding a time threshold without having detected an expected portion of the 802.1x authentication sequence do not

occur; the detection component having identified the wireless network as a 802.1x attempting a wireless provisioning services sequence and determining that the wireless network does not support wireless provisioning when a failure of a portion of the wireless provisioning services authentication sequence or exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence occurs; and, the detection component identifying the wireless network as a 802.1x supporting wireless provisioning services network when a failure of a portion of the wireless provisioning services authentication sequence and exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence do not occur.

Ayyagrari et al discloses a system for switching between available networks as a user moves to different locations without the user having to manually enter network connection information upon arrival at each location. This is accomplished by the system caching information when a user enters information the first time or providing a UI for the user to enter information for networks in advance as stored network preferences. The system employs beacon information received/downloaded from the network to identify available networks and uses the cached or stored information to connect to the known networks. If there are no known networks the system attempts to connect to ad hoc networks. When the system attempts to connect to a network and the connection fails, the system attempts to connect to a different network.

He et al discloses a system for managing secured access to network resources using a general ticket that is issued upon a first authentication of the user and is reused

for subsequent requests. The cited section refers to use of a Kerberos authentication security as the general ticket server for a dial-up server. Upon a failure of the Kerberos server or a server timeout, the system switches the user to a dial-up access to the network. In this scenario, the security mechanisms are known to the server and there is no identification of encryption types being performed.

Krantz et al discloses a system for allowing a user to connect to an ISP without requiring the user to have any previous knowledge about the requirements or have to call the ISP to connect to the ISP network. This is accomplished by redirecting the user to a URI that downloads a master document, which contains information regarding the connection requirements for an ISP, or by having this information pre-stored on the user's computer.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FATOUMATA TRAORE whose telephone number is (571)270-1685. The examiner can normally be reached on Monday- Friday (every other Friday off) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on 571 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436